PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : H04L 9/00 — A1

(11) International Publication Number: WO 00/62472

(43) International Publication Date: 19 October 2000 (19.10.00)

(21) International Application Number: PCT/US00/05135

(22) International Filing Date: 29 February 2000 (29.02.00)

(30) Priority Data:
09/288,412 8 April 1999 (08.04.99) US

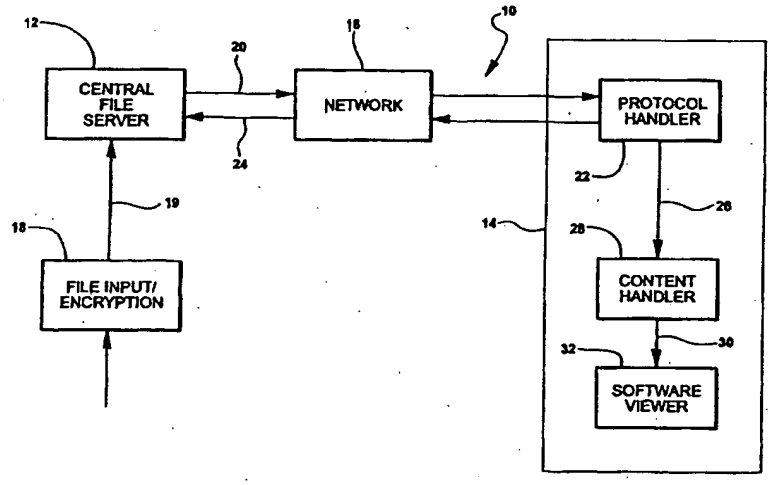
(71)(72) Applicant and Inventor: BLUM, James, M. [US/US]; 4566 Middleton, West Bloomfield, MI 48323 (US).

(74) Agents: MCEVOY, Douglas, J. et al.; Gifford, Krass, Groh, Sprinkle, Anderson & Citkowski, P.C., 280 N. Old Woodward, Suite 400, Birmingham, MI 48009 (US).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: SYSTEM AND METHOD FOR TRANSMISSION OF ENCRYPTED FILES FROM A CENTRAL SERVER COMPUTER TO A REMOTE COMPUTER



(57) Abstract

A system, described in reference to the figure, for providing secure transmission of an encrypted file over a computer network (16) having a central file server (12) operatively connected through a communication line with a remotely located client server (14). A data encryption and input unit (18) operatively connected to the central file server (12) and capable of receiving and encrypting a plurality of files. The central file server (12) uploads selected pre–encrypted files from the encryption and input unit (18). The remote server includes a protocol handler (22) which utilizes an existing protocol to spoof the central file server (12) to transmit selected files in an encrypted form to the remote server (14). The protocol functions then to algorithmically decrypt the files by generically modifying the incoming data associated with the file and a content handler (28) connected (26) to the protocol handler (22) then forwards (30) the modified data to a pre–loaded software program for opening and presentation.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

SYSTEM AND METHOD FOR TRANSMISSION OF ENCRYPTED FILES FROM A CENTRAL SERVER COMPUTER TO A REMOTE COMPUTER

Background of the Invention

Field of the Invention

The present invention relates generally to data encryption systems and techniques and, more particularly, to a system for providing secure transmission of encrypted files from a central server computer to a remote computer and method for practicing the same and which utilizes existing protocols, servers and clients.

Description of the Prior Art

The use of Internet technologies for delivering various types of data content has increased dramatically in the past few years. Public networks have made the electronic transfer of data between organizations relatively simple. However, with the simplicity comes great security risks. Numerous solutions have been proposed for securing data during its transmission over a network, such as various encryption schemes, and the result of which is the existence of a burgeoning amount of Internet commerce. Additionally, much of this data delivery has spawned the creation of customized client/server combinations or content-handling programs to view data files and it has been found that the continual creation of software to provide access to new types of data, and in particular encrypted data, becomes very inefficient.

According to existing systems, data is uploaded to a central file server in unencrypted form and prior to subsequent encryption and transmission over a network to a remote server. Typically, a protocol handler at the remote client location or server requests a file over the network from the central server. The file is requested from the server and the server responds with the file and a MIME type.

Upon receiving the encrypted file, the protocol handler forwards the data within the file to a content handler unit. The content handler typically employs one or more decryption programs for algorithmically decrypting the specific types of transferred file, such as the graphic, text and audio components for subsequent display by another program. The content handler may further be built into the network browser or function as a stand alone unit. A number of different MIME types are defined to execute the appropriate content handler.

The drawbacks of such conventional encryption systems include that the file must be recognized as encrypted and forwarded on to an encryption program. After decryption, the file must again be recognized to launch the proper viewing software. This type of identification is very inconsistent and often encryption programs do not maintain information about the type of data being encrypted. The user is typically then left with the burden of determining what type of data is actually encrypted and/or this then involves having to utilize a special server and a special piece of client software for decrypting a file.

A further drawback includes having to integrate data from several sources or different types of data onto one screen. As an example, if a World Wide Web browser needs to display a encrypted graphic, some text, and a video clip, current technology would not enable this to occur. The only solution would then be to define specific MIME types for the encrypted version of each media type and write decrypting content handlers for each type. This results in a doubling of the number of content handlers required and attendant amount of extra code that needs to be developed to facilitate such functionality. A further evident shortcoming of the existing system is the danger of maintaining files in unencrypted form on the central file server and prior to subsequent encryption and transmission, such danger arising in the form of data theft from employees, contractors and other persons having access to the central server.

Summary of the Present Invention

The present invention provides a system for providing secure transmission of an encrypted file over a computer network and which is a marked improvement over the above-described prior art. According to the present invention, a data encryption and input unit is operatively connected to the central file server for inputting and encrypting the files prior to them being stored in the central server. This is accomplished utilizing any conventional encrypting algorithm and enabling the central server to call up selected files.

A protocol handler is operatively connected to a remotely located client or server and functions to request the encrypted file or files to be transmitted from the central server. The protocol handler specifically sends its request utilizing an existing network protocol and in effect "spoofs" the central server into sending data to the client which is in effect stored in the central server as if it was not encrypted and with the same type labeling as an unencrypted file. The effect of "spoofing" the central server causes the protocol handler to generically modify the incoming data (the equivalent of decryption) and thus providing a key decryption function which is otherwise reserved to the prior art systems. The protocol handler further is capable of modifying the data in this instance in such a way that it provides previously existing content types to the content-handling algorithm of the client.

Using this system, any type of data can be encrypted and displayed if the original type of data can be displayed. All existing content handlers will function normally because they are dealing with unencrypted data when they are called. The result is that the protocol handler essentially substitutes for the functions of the content handler previously provided by the content handler in decrypting the files and provides for an attendant reduction in necessary software code and more efficient opening and viewing of the decrypted files. This is so because the need for specialized servers and content-handlers is eliminated through the protocol spoofing function.

Brief Description of the Drawings

Reference will now be made to the attached drawings, when read in combination with the following specification, wherein like reference numerals refer to like parts throughout the several views, and in which:

Fig. 1 is a schematic view of the system for providing secure transmission of an encrypted file over a computer network according to the present invention.

Detailed Description of the Preferred Embodiment

Referring now to Fig. 1, a system for providing secure storage and transmission of an encrypted file over a computer network is illustrated at 10 according to the present invention. A central file server 12 according to known construction is operably connected through a communication line to a remotely located client or server 14. The remote client 14 can qualify as any PC computer or the like. A network connection, illustrated schematically at 16, is known in the art and is capable of operably connecting the central file server 12 with a plurality of individually located and remote client's or servers.

A data encryption and input unit 18 is operably connected to the central file server 12 and is capable of receiving and encrypting a plurality of files prior to uploading to the central server 12. As was previously discussed, it is advantageous to encrypt files prior to uploading to the central server in order to prevent unauthorized access or tampering by internal personnel at the central location.

The procedure for calling up and transmitting encrypted files from the central server as diagrammatically illustrated in Fig. 1 includes the step of the central server 12 first communicating along a line 20 across a network and to selected remote server 14. As is known in the art, a central server 12 could typically connect to large pluralities of remote client servers, however only a single server is illustrated for convenience sake.

The data is encrypted and stored on the central file server 12 in a format consistent as if it was not encrypted and with the same type labeling as

an unencrypted file, particularly such as in a hyper text transmission protocol (http) or a file transfer protocol (ftp). Forming an integral part of the client, or forming a separated and connected part, is a protocol handler 22 which functions to request, through the network 16, a selected file or files from the central server 12. This is accomplished by the protocol handler 22 making a request for information using a locally defined network protocol and sending the request along a communication line defined at 24 extending from the protocol handler 22, through the network 16 and to the central file server 12. The request thus invokes a new protocol-handler and in effect "spoofs" the central server 12 into sending the encrypted data, labeled in unencrypted form, to the client.

The protocol handler 22, once it receives the encrypted data through the remote server 14 and via line 20, algorithmically decrypts the data generically modifying the data in such a way that it provides previously existing content. The trigger used to open encrypted files is the relabeling of an existing protocol handler. As an example, a HTTP protocol could be relabeled as MDRP and would still connect to the server using standard HTTP protocol. Likewise, a FTP protocol may be employed. However, when the data is received, the type of encryption, if any, would be determined by the client's protocol handler.

A single protocol handler decrypts all possible data types and then sends the unencrypted files, via a line 26, to a content handler 28 operably connected thereto which determines the type of data utilizing one or more MIME types and then forwards the data, via a further line 30, to another software program and viewer 32 for opening the file. By utilizing protocol spoofing the one protocol handler eliminates the need for many separate content handlers and MIME types.

Manifestations of the above-described system include the design of prototype health information systems which model a method to provide access to medical records over the Internet. Also, the technique of protocol spoofing could also be used for data conversion or any other types of systems which

involve the application of a standard algorithm. For example, a compression algorithm that saves space on a file server could be implemented in a spoofing protocol handler. The data would be stored in a compressed fashion possibly using an uploading spoofing protocol handler. The data could then be retrieved using the same protocol handler with the complementary decompression algorithm.

A method of providing for secure transmission of an encrypted file utilizing the system according to the present invention is also disclosed and includes the steps of loading the selected file or files into a data encryption and input unit which is operatively connected to the central file server and encrypting the file according to any conventionally known procedure. Additional steps include the protocol handler requesting transmission of the file over the network utilizing an existing protocol and decrypting the file through generically modifying the incoming data and transferring the decrypted file to a content handler for subsequent presentation by a software viewer.

Having described my invention, additional preferred embodiments will become apparent to those skilled in the art to which it pertains without deviating from the scope of the appended claims.

I claim:

Claims

1. A system for providing secure transmission of an encrypted file over a computer network, said system comprising:

a central file server;

said central file server operably connecting through a communication line with a remotely located server;

a data encryption and input unit operably connected to said central file server and capable of receiving and encrypting a plurality of files;

said central file server uploading selected pre-encrypted files from said encryption and input unit;

said remote server further including a protocol handler operably connected thereto, said protocol handler requesting at least one of said plurality of encrypted files using a standardized protocol to be transmitted from said central file server;

said protocol handler decrypting said at least one file by generically modifying incoming data associated with said file; and

a content handler operably connected to said protocol handler and receiving said decrypted file, said content handler forwarding said modified data to a pre-loaded software program for subsequent display.

2. The system as described in claim 1, further comprising said data being stored in said central file server utilizing an identical type labeling as a corresponding unencrypted file.

3. The system as described in claim 1, further comprising said content handler determining the type of data sent by said protocol handler utilizing one or more MIME types.

4. The system as described in claim 1, further comprising said protocol handler being capable of decrypting all data types.

5. The system as described in claim 4, said standardized protocol further comprising an HTTP protocol.

6. The system as described in claim 4, said standardized protocol further comprising a FTP protocol.

7. The system as described in claim 1, further comprising said protocol handler algorithmically decrypting said at least one file through the use of one or more keys.

8. A method for providing secure transmission of an encrypted file over a computer network, comprising the steps of:

loading a selected file into a data encryption and input unit which is operatively connected to a central file server;

encrypting said selected file within said encryption and input unit and uploading said file into said central file server;

requesting said encrypted file for transmission over the network from a protocol handler operatively communicating with said remote server and utilizing an existing protocol to obtain said encrypted files;

decrypting said file through said protocol handler utilizing a private key and by generically modifying the incoming data associated with said file; and

transferring said decrypted file to a content handler operatively connected to the protocol handler for forwarding to a software viewer for opening and presentation.

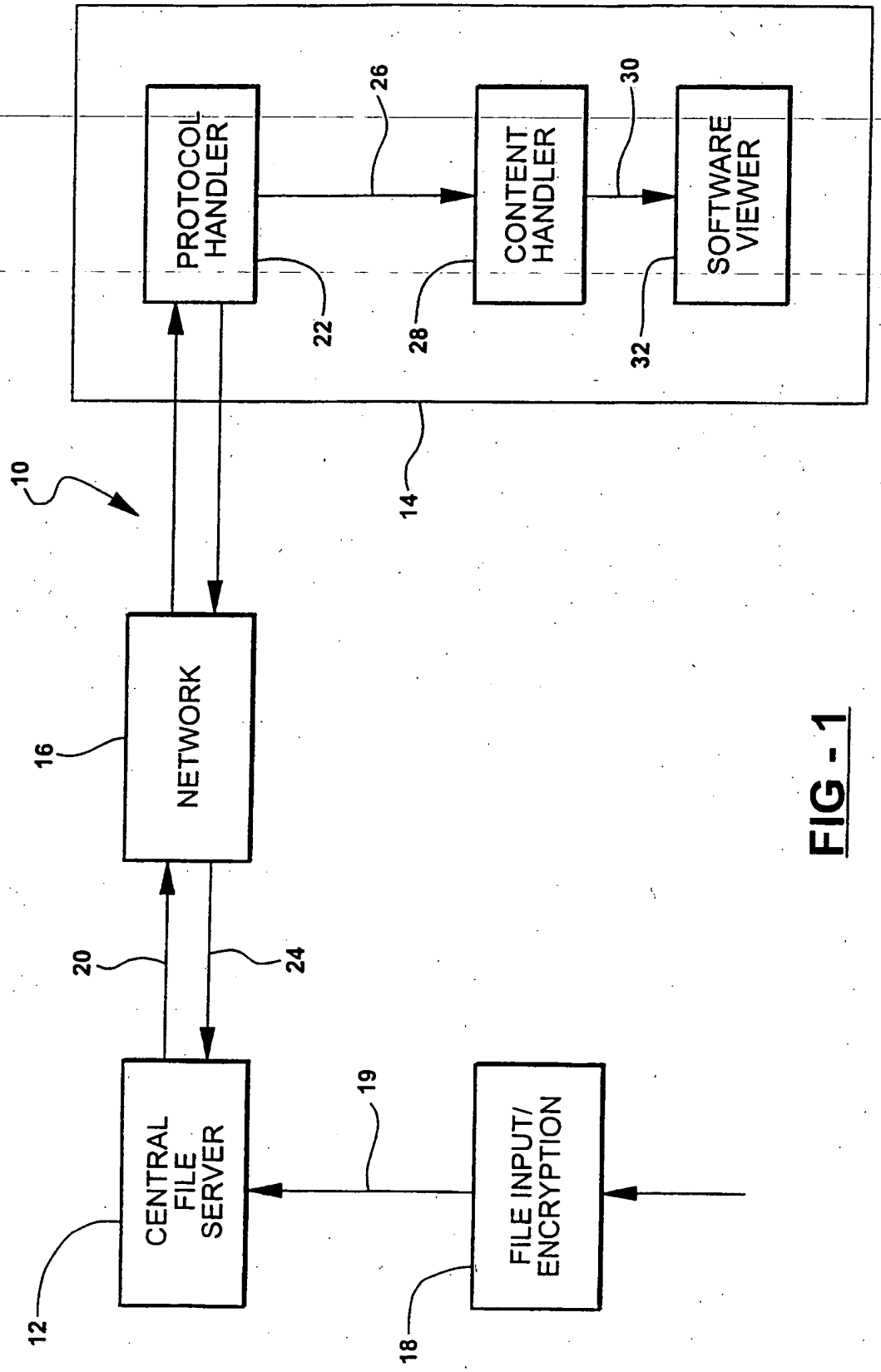

PROTOCOL HANDLER
CONTENT HANDLER
SOFTWARE VIEWER
NETWORK
CENTRAL FILE SERVER
FILE INPUT/ ENCRYPTION
10
12
14
16
18
19
20
22
24
26
28
30
32

FIG - 1

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/05135

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) : H04L 9/00

US CL : 713/151

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 713/151, 153, 154; 380/269

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Inventor name searches conducted on Dialog and STN CAS

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,719,938 A (HAAS et al.) 17 February 1998, column 3, lines 23-46 and column 4, lines 7-17.	1-8
Y	US 5,881,287 A (MAST) 09 March 1999, column 8 lines 45-60.	2
Y	TANENBAUM, A. S. Computer Networks. Third Edition. Prentice Hall. 1996. Pages 3-17, 16-38, 681-691.	1-8

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
	11 JUL 2000
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703)305-3230	Authorized officer Gail O. Hayes James R. Matthews Telephone No. (703) 305-3900

Form PCT/ISA/210 (second sheet) (July 1998)